Notice of Allowability	Application No.	Applicant(s)	
	09/591,927	MIURA ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the communication filed on February 22, 2005*.

2. ☒ The allowed claim(s) is/are *1,4,5,8-11,13,14,16,18-22,24 and 25*.

3. ☒ The drawings filed on *12 June 2000* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *5/10/05* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CAR
5/10/05

NOTICE OF ALLOWANCE

Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with George Yee on May 10, 2005.

The application has been amended as follows:

1. (Currently Amended) An electronic authentication method comprising:

in a first information processing apparatus, receiving a request for contents from a second information processing apparatus;

in response to said request, generating an encryption key and an access number that are associated with said requested contents;

producing enhanced content comprising said requested contents, said encryption key, and said access number:

transmitting said enhanced content to said second information processing apparatus;

presenting said enhanced content to a user at said second information processing apparatus, said encryption key and said access number are visually imperceptible to a user;

in said second information processing apparatus, accessing said encryption key and said access number from said enhanced content;

receiving [user] data in said second information processing apparatus and in response thereto producing input data from said [user] received data that includes the transmitted access number, wherein at least some of said input data is encrypted with said encryption key [, said]; and

transmitting said input data from said second information apparatus to said first information apparatus as received input data,

wherein said first information processing apparatus can authenticate legitimacy of said received input data based on said access number.

5. (Currently Amended): An information processing method comprising:

generating an encryption key and an access number that are associated with contents;

creating an access information record corresponding to said encryption key and said access number;

incorporating said encryption key and said access number into said contents to produce enhanced contents, said encryption key and said access number are visually imperceptible to a user;

transmitting said enhanced contents to an external apparatus;

receiving received data from said external apparatus, said received data including said [a user-provided] access number, at least a portion of said received data being encrypted with said encryption key;

decrypting said received data; and

deleting said access information record based on whether said received data could be decrypted and based on a comparison with said access number and said [user-provided] received data including said access number.

8. (Currently Amended) An electronic authentication system comprising a first information processing apparatus and a second information processing apparatus wherein:

said first information processing apparatus comprises:

a means for generating an encryption key and an access number associated with first contents;

a storage means for storing a record that corresponds to said encryption key and said access number;

a means for transmitting enhanced contents to said second information processing apparatus, said enhanced contents comprising said first contents, said encryption key, and said access number, said encryption key and said access number are visually imperceptible to a user;

said second information processing apparatus comprises:

a means for inputting [user] the received data, including means for displaying received enhanced contents; [and]

a means for transmitting said [user] received data [and said identifier] to said first information processing apparatus as input data, wherein said input data is generated by encrypting said [user] data and includes said access number; and

there is further provided in said first information processing apparatus a processing means for authenticating legitimacy of said input data received by said first information processing apparatus and deleting said record based at least on a comparison of said stored access number and said access number contained in said received input data.

11. (Currently amended) An information processing apparatus comprising:

a generation means for generating an identifier for contents, said identifier comprising and encryption key and an access number;

a storage means for storing at least said first part of said identifier as a stored identifier;

a transmission means for transmitting enhanced content comprising said contents and said identifier to an external apparatus, said encryption key and said access number are visually imperceptible to a user;

a reception means for receiving received data from said external apparatus, said received data comprising a [user-provided] access number and a portion that has been encrypted using said encryption key;

an acquirement means for acquiring [user-provided] said access number from said received data; and

a processing means for deleting said stored identifier if said [user-provided] access number matches said stored access number.

14. (Currently amended) An information processing apparatus comprising:

a contents requesting means for requesting an external information processing apparatus to transmit contents;

a reception means for receiving said requested contents, an identifier comprising an encryption key and an access number being embedded in said requested contents;

a display means for displaying said requested contents to a user, said encryption key and said access number are visually imperceptible to a user;

an extraction means for extracting said identifier from said requested contents;

an input means for inputting said access number [user data from a user]; and

a transmission means for transmitting, as secured data, said [user data and said] access number to said external information processing apparatus, at least of portion of said secured data being encrypted by said encryption key ; and

means for said external information processing apparatus to authenticate legitimacy of said received access number.

16. (Currently amended) A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a generation function for generating an encryption key and an access number for first contents;

a storage function for storing a stored identifier corresponding to said encryption key and said access number;

a transmission function for transmitting said contents, said identifier, and said access number to an external apparatus as enhanced content, said encryption key and said access number are visually imperceptible to a user;

a reception function for receiving received data from said external apparatus, said received data comprising [a user-provided] said access number and a portion that is encrypted using said encryption key;

an acquirement function for acquiring said [user-provided] access number from said received data; and

a processing function for authenticating legitimacy of said received data and invalidating said stored identifier if said [user-provided] received access number matches stored access number.

19. (Currently amended) A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a contents requesting function for requesting an external information processing apparatus to transmit contents;

a reception function for receiving said requested contents, an identifier being embedded in said contents, said identifier comprising an encryption key and an access number;

a display function for displaying said requested contents to a user, said encryption key and said access number are visually imperceptible to a user;

an extraction function for extracting said identifier from said contents;

an input function for inputting said access number [user data from a user]; and

a transmission function for transmitting, as input data, [said user data] said access number to said external information processing apparatus, a portion of said input data being encrypted using said encryption key; and

said external information processing apparatus authenticates the legitimacy of said received access number.

21. (Currently amended): An electronic authentication method comprising:

generating an identifier for contents in a first information processing apparatus, said identifier comprising an encryption key and an access number;

driving said first information processing apparatus to store at least a first portion of said identifier and the present time as a storage time in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus as enhanced content, wherein said identifier is embedded in said contents;

presenting said enhanced content to a user at said second information processing apparatus, said encryption key and said access number are visually imperceptible to a user;

inputting [user data] said access number in said second information processing apparatus;

transmitting, as secured data, [said user data and] said access number contained in said enhanced content from said second information processing apparatus to said first information processing apparatus, a portion of said secured data encrypted by said encryption key contained in said enhanced content; and

invalidating said first portion of said identifier stored in said storage unit if said identifier received by said first information processing apparatus is not stored in said storage unit or a time of a predetermined length has lapsed since said storage time stored in said storage unit.

22. (Currently amended) An electronic authentication method, comprising:

generating an encryption key and an access number that are associated with contents in a first information processing apparatus;

embedding said encryption key and said access number into said contents to produce enhanced content, said encryption key and said access number are visually imperceptible to a user;

transmitting said enhanced content to a second information processing apparatus;

displaying said enhanced content in said second information processing apparatus;

inputting [user data] said access number in said second information processing apparatus;

obtaining said access number from said enhanced data;

encrypting [said user data] said access number using said encryption key to produce secured input data, including acquiring said encryption key from said enhanced content;

transmitting said secured input data and said access number from said second information processing apparatus to said first information processing apparatus; and

validating said secured input data based on said access number and by decrypting said secured input data with a decryption key.

24. (Currently amended) An authentication method in a system in which a first computer making a request for a service is connected to a second computer rendering services via a network, requested contents being transmitted from the second computer to the first computer, data being transmitted from the first computer to the second computer associated with the contents, said method comprising:

generating at the second computer an encryption key relating to the contents;

generating at the second computer an access number for accessing the contents and cataloging the access number in a storage unit;

embedding the encryption key and the access number in the contents to produce enhanced content, said encryption key and said access number are visually imperceptible to a user, and transmitting the enhanced content to the first computer;

displaying the contents at the first computer;

generating secured data at the first computer by processing [user-provided data with] the access number fetched from the enhanced content and transmitting the secured data to the second computer, some of the secured data being encrypted with the encryption key fetched from the enhanced content; and

at the second computer authenticating validity of the secured data based on the access number in the secured data and by decrypting the secured data with a decryption key.

Reasons for Allowance

2. The following is an examiner's statement of reasons for allowance:

According to the applicant's specification, there exists embodiments whereby a browser program is responsible for retrieving an encryption key and access number that is embedded in an image, wherein the encryption key and access number are not visible to a user, and the browser program is responsible for retrieval of the encryption key and access number and further encrypts the access number with the encryption for transmission to a server or external party for verification according to the applicant's specification recited on page 2, lines 23-29; page 6, lines 19-25; page 7, lines 26-30;

and page 8, lines 4-10. Prior art techniques are responsible for requiring a user to enter the password and which is then encrypted and sent for verification.

It was not found to be taught in the prior art of sending a second system/external apparatus an encryption key and an access number, such that the encryption key and access number are visually imperceptible to a user. The second party/external apparatus encrypts the access number with the encryption key and returns this information and it is determined if they compare/authenticate/match.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The Colvin Patents disclose of an encrypted password that is transmitted to a user in order to gain access and usage of software.

Kawamura et al, U.S. Patent 6,519,701 discloses of storing authentication data that includes an identification number unique to and information processing apparatus and a license key that includes an encryption key.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

5/10/05

CR

May 10, 2005